บริษัท ทรีคอม เอเชีย จำกัด

อินเทอร์เน็ตไฟร์วอลล์ กับการรักษาความปลอดภัย

การรักษาความปลอดภัย กลายเป็นเรื่องหลักที่ควรพิจารณา เมื่อองค์กรต่อเชื่อมเครือข่ายส่วนตัว เข้ากับอินเทอร์เน็ต

จำนวนผู้ใช้บนเครือข่ายเอกเทศที่ต้องการเข้าถึงบริการของอินเทอร์เน็ต เช่น World-Wide Web (WWW), Internet Mail, Telnet, และ File Transfer Protocol (FTP) กำลังเพิ่มขึ้นอยู่ตลอดเวลา นอกจากนั้นบริษัทต่าง ๆ ยังต้องการเสนอโฮมเพจของ WWW และเซอร์ฟเวอร์ FTP สำหรับให้เข้าถึงได้โดยสาธารณะผ่านทางอินเทอร์เน็ตอีกด้วย ผู้ดูแลเครือข่ายกังวลเกี่ยวกับการรักษาความปลอดภัยของเครือข่ายมากขึ้นเมื่อพวกเขาเปิดเผยข้อมูลส่วนตัวและโครงสร้างพื้นฐานการทำเครือข่ายขององค์กรไปบนความเปราะบางของอินเทอร์เน็ต เพื่อให้มีการปกป้องในระดับที่ต้องการ องค์กรต้องมีนโยบายการรักษาความปลอดภัยที่จะป้องกันมิให้ผู้ใช้ซึ่งไม่ได้รับอนุญาตเข้าถึงทรัพยากรบนเครือข่ายส่วนตัว และเพื่อปกป้องไม่ให้มีการเผยแพร่ข้อมูลออกไปโดยไม่ได้รับอนุญาต แม้ว่าองค์กรจะไม่ได้ต่อเชื่อมกับอินเทอร์เน็ตก็ตาม การสร้างนโยบายการรักษาความปลอดภัยภายในก็อาจเป็นสิ่งจำเป็นเพื่อจัดการผู้ใช้ในการเข้าถึงส่วนต่าง ๆ ของเครือข่าย และเพื่อปกป้องข้อมูลที่อ่อนไหวหรือเป็นความลับ

อินเทอร์เน็ตไฟร์วอลล์

อินเทอร์เน็ตไฟร์วอลล์ (Internet Firewall) เป็นระบบหรือกลุ่มของระบบป้องกันที่บังคับใช้นโยบายการรักษาความปลอดภัยระหว่างเครือข่ายขององค์กรกับอินเทอร์เน็ต ไฟร์วอลล์เป็นตัวกำหนดว่าบริการภายในชนิดใดบ้างที่อาจเข้าถึงได้จากภายนอก ผู้ใช้ภายนอกคนใดที่ได้รับอนุญาตให้เข้าถึงบริการภายในที่ยอมให้ใช้ และบริการภายนอกใดที่อาจเข้าถึงได้โดยผู้ใช้ภายใน เพื่อให้ไฟร์วอลล์มีประสิทธิผล การจราจรของข้อมูลทั้งหมดที่ผ่านเข้าออกอินเทอร์เน็ตจะต้องผ่านไฟร์วอลล์ ซึ่งเป็นด่านสำหรับตรวจสอบข้อมูล ไฟร์วอลล์จะยอมให้ผ่านเฉพาะข้อมูลที่ได้รับอนุญาตเท่านั้น และตัวไฟร์วอลล์เองต้องปลอดจากการบุกรุก ระบบไฟร์วอลล์ไม่สามารถปกป้องสิ่งใดหากผู้โจมตีผ่านไฟร์วอลล์เข้ามาได้

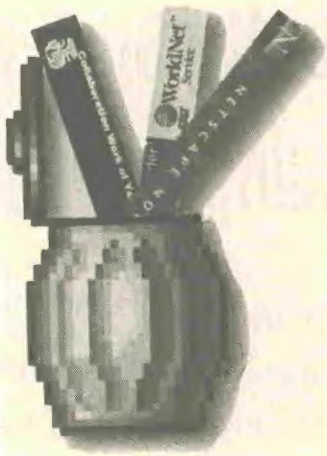
อินเทอร์เน็ตไฟร์วอลล์ไม่ใช่แค่เราเตอร์ (router) แบสชันโฮสต์ (bastion host) หรืออุปกรณ์ที่มาประกอบกันเพื่อการรักษาความปลอดภัยเครือข่าย ไฟร์วอลล์เป็นส่วนหนึ่งของ

นโยบายการรักษาความปลอดภัยทั้งหมดที่ก่อขึ้นเป็นแนวป้องกันซึ่งถูกออกแบบสำหรับปกป้องทรัพยากรสารสนเทศขององค์กร นโยบายการรักษาความปลอดภัยนี้ต้องรวมถึงแนวทางการรักษาความปลอดภัยที่พิมพ์เผยแพร่แก่ผู้ใช้ในความรับผิดชอบ เช่น นโยบายของบริษัทที่กำหนดการเข้าถึงเครือข่าย การเข้าถึงบริการ การตรวจสอบผู้ใช้โลคอลและรีโมท การโทรเข้าและโทรออก การเข้ารหัสลับข้อมูล และการป้องกันไวรัส รวมถึงการฝึกอบรมพนักงาน ทุกจุดของเครือข่ายที่มีสิทธิ์ถูกโจมตีต้องถูกปกป้องด้วยการรักษาความปลอดภัยในระดับเดียวกัน การตั้งอินเทอร์เน็ตไฟร์วอลล์โดยปราศจากนโยบายการรักษาความปลอดภัยอย่างครบถ้วนก็เหมือนกับการใส่ประตูเหล็กให้กับกระโจม

ประโยชน์ของอินเทอร์เน็ตไฟร์วอลล์

อินเทอร์เน็ตไฟร์วอลล์จัดการการเข้าถึงระหว่างอินเทอร์เน็ตและเครือข่ายส่วนตัวขององค์กร หากปราศจากไฟร์วอลล์ ระบบโฮสต์แต่ละระบบบนเครือข่ายส่วนตัวจะเปิดกว้างต่อการโจมตีจากโฮสต์อื่นบนอินเทอร์เน็ต หมายความว่าการรักษาความปลอดภัยของเครือข่ายส่วนตัวจะขึ้นอยู่กับความแข็งแกร่งของคุณสมบัติการรักษาความปลอดภัยของโฮสต์แต่ละเครื่อง และจะปลอดภัยเท่ากับระบบที่อ่อนแอที่สุดเท่านั้น

อินเทอร์เน็ตไฟร์วอลล์ยอมให้ผู้ดูแลเครือข่ายกำหนด "จุดสกัด" ที่คอยระวังผู้ใช้ซึ่งไม่ได้รับอนุญาต เช่น แฮกเกอร์ (hacker) แครกเกอร์ (cracker) แวนดัล (vandal) และสปาย (spy) ออกจากเครือข่ายซึ่งได้รับการปกป้อง ห้ามไม่ให้บริการที่เปราะบางเข้าสู่หรือออกจากเครือข่ายซึ่งได้รับการปกป้อง และให้การคุ้มครองจากการโจมตีผ่านเราติงแบบต่างๆ อินเทอร์เน็ตไฟร์วอลล์ทำให้การจัดการรักษาความปลอดภัยง่ายขึ้น เนื่องจากการรักษาความ



ปลอดภัยเครือข่ายถูกรวมไว้บนระบบไฟร์วอลล์แทนการกระจายไปบนโฮสต์ทุกตัวในเครือข่ายส่วนตัวทั้งเครือข่าย

ไฟร์วอลล์ให้ความสะดวกในการเฝ้าคุมการรักษาความปลอดภัยของอินเทอร์เน็ตและการแจ้งเตือน ควรสังเกตว่าสำหรับองค์กรที่มีการเชื่อมต่อกับอินเทอร์เน็ต ปัญหาไม่ใช่ว่าการโจมตีจะเกิดขึ้นหรือไม่ แต่เป็นเมื่อใดจะเกิดขึ้น ผู้ดูแลเครือข่ายต้องตรวจสอบและบันทึกการจราจรของข้อมูลซึ่งมีนัยสำคัญทั้งหมดที่ผ่านไฟร์วอลล์ ถ้าผู้ดูแลเครือข่ายไม่ใช้เวลาเพื่อตอบสนองต่อการแจ้งเตือนและตรวจสอบบันทึกอย่างสม่ำเสมอ ก็ไม่มีความจำเป็นต้องใช้ไฟร์วอลล์ เพราะผู้ดูแลเครือข่ายจะไม่เคยรู้ว่าไฟร์วอลล์ได้ถูกโจมตีสำเร็จไปแล้วหรือไม่

เมื่อ 2-3 ปีก่อน อินเทอร์เน็ตได้เผชิญกับวิกฤตการณ์ของจำนวนแอดเดรสซึ่งทำให้ IP แอดเดรสที่ลงทะเบียนเป็นทรัพยากรที่เหลือน้อยมาก หมายความว่าองค์กรที่ต้องการเชื่อมต่อกับอินเทอร์เน็ตอาจได้รับ IP แอดเดรสไม่เพียงพอกับความต้องการที่เพิ่มขึ้นตามจำนวนผู้ใช้ อินเทอร์เน็ตไฟร์วอลล์เป็นตำแหน่งที่เหมาะสมสำหรับจัดการกับ Network Address Translator (NAT) ซึ่งสามารถช่วยบรรเทาการขาดแคลนจำนวนแอดเดรส และกำจัดความจำเป็นที่ต้องจัดหมายเลขใหม่เมื่อองค์กรเปลี่ยนผู้ให้บริการอินเทอร์เน็ต (Internet Service Providers - ISP)

อินเทอร์เน็ตไฟร์วอลล์เป็นจุดซึ่งเหมาะสมที่สุดสำหรับการตรวจสอบหรือบันทึกการใช้งานอินเทอร์เน็ต วิธีนี้ทำให้ผู้ดูแลเครือข่ายสามารถรู้ค่าใช้จ่ายของการเชื่อมต่ออินเทอร์เน็ตเพื่อการจัดการกับปัญหาคอขวดของแบนด์วิดธ์ และคิดค่าใช้จ่ายกับแผนกที่ใช้งานหากเข้ากันได้กับโครงสร้างทางการเงินขององค์กร

อินเทอร์เน็ตไฟร์วอลล์ยังเสนอจุดศูนย์กลางของการติดต่อสำหรับบริการจัดส่งข้อมูลไปยังลูกค้าอีกด้วย อินเทอร์เน็ตไฟร์วอลล์เป็นตำแหน่งในอุดมคติสำหรับการจัดตำแหน่งเซอร์ฟเวอร์ World-Wide Web และ FTP ไฟร์วอลล์สามารถถูกปรับตั้งเพื่ออนุญาตให้เข้าถึงบริการเหล่านี้ผ่านอินเทอร์เน็ต ขณะที่ป้องกันการเข้าถึงระบบอื่นบนเครือข่ายส่วนตัวจากภายนอก

ท้ายที่สุด บางคนอาจแย้งว่าการจัดตำแหน่งของอินเทอร์เน็ตไฟร์วอลล์ทำให้เกิดความล้มเหลวได้จากจุดเดียว ควรจะต้องเน้นให้เห็นว่า ถ้าการเชื่อมต่อกับอินเทอร์เน็ตล้มเหลว เครือข่ายส่วนตัวขององค์กรจะยังปฏิบัติงานได้ต่อไป มีเพียงการเข้าถึงอินเทอร์เน็ตเท่านั้นที่ทำไม่ได้ ถ้ามีจุดเข้าถึงหลายจุด แต่ละจุดจะกลายเป็นจุดที่อาจถูกโจมตี ซึ่งผู้ดูแลเครือข่ายต้องจำกัดความเสียหายและเฝ้าคุมอย่างสม่ำเสมอ

ข้อจำกัดของอินเทอร์เน็ตไฟร์วอลล์

อินเทอร์เน็ตไฟร์วอลล์ไม่สามารถปกป้องการโจมตีที่ไม่ได้ผ่านไฟร์วอลล์ ตัวอย่างเช่น ถ้ามีการโทรออกอย่างไม่มีข้อจำกัดจากภายในเครือข่ายที่ได้รับการป้องกัน ผู้ใช้ภายในจะสามารถสร้างการเชื่อมต่อด้วย SLIP หรือ PPP ไปยังอินเทอร์เน็ตได้โดยตรง ผู้ใช้ซึ่งมีความรู้และไม่พอใจกับการตรวจสอบเพิ่มเติมโดยพรอกซีเซอร์ฟเวอร์ (proxy server) ของไฟร์วอลล์ อาจมีความรู้สึกอยากหลบหลีก

ระบบรักษาความปลอดภัยด้วยการซื้อการเชื่อมต่อแบบ SLIP หรือ PPP โดยตรงไปยัง ISP เนื่องจากการเชื่อมต่อประเภทนี้ไม่ผ่านระบบรักษาความปลอดภัยของไฟร์วอลล์ที่สร้างอย่างรอบคอบที่สุด พวกมันจึงล่อแหลมต่อการโจมตีทางประตูหลัง (back door) ผู้ใช้ต้องตระหนักว่าการเชื่อมต่อประเภทนี้ไม่ได้รับอนุญาตให้เป็นส่วนหนึ่งของสถาปัตยกรรมระบบรักษาความปลอดภัยโดยรวมขององค์กร

อินเทอร์เน็ตไฟร์วอลล์ไม่สามารถป้องกันการก่อกวนจากผู้ทรยศหรือผู้ใช้ที่ไม่ตั้งใจ ไฟร์วอลล์ไม่ได้ห้ามผู้ทรยศหรือสายลับธุรกิจจากการคัดลอกข้อมูลที่อ่อนไหวไปยังฟลอปปี้ดิสค์หรือการ์ด PCMCIA และนำออกไปจากอาคาร ไฟร์วอลล์ไม่ได้ปกป้องการโจมตีที่แฮกเกอร์ปลอมเป็นผู้ดูแล (supervisor) หรือพนักงานใหม่ที่ไม่รู้ประสีประสา แล้วไปหลอกลวงผู้ใช้ที่ไม่ทันคนให้เปิดเผยรหัสผ่านหรือให้สิทธิพวกเขาเข้าถึงเครือข่ายชั่วคราว พนักงานต้องได้รับการสอนเกี่ยวกับการโจมตีประเภทต่าง ๆ และเกี่ยวกับความจำเป็นต้องป้องกันและเปลี่ยนแปลงรหัสผ่านของพวกเขาเป็นระยะ

อินเทอร์เน็ตไฟร์วอลล์ไม่สามารถป้องกันการถ่ายโอนไฟล์หรือซอฟต์แวร์ที่ติดไวรัส เนื่องจากมีไวรัส ระบบปฏิบัติการ และวิธีการเข้ารหัสและบีบอัดไบนารีไฟล์ที่แตกต่างกันเป็นจำนวนมาก จึงไม่อาจคาดหวังได้ว่าอินเทอร์เน็ตไฟร์วอลล์จะตรวจสอบการติดไวรัสในทุกไฟล์ได้อย่างแม่นยำ องค์กรที่เป็นห่วงควรจัดให้มีซอฟต์แวร์ป้องกันไวรัสในเดสค์ท็อปแต่ละเครื่องเพื่อปกป้องจากไวรัสที่มากับฟลอปปี้ดิสค์หรือแหล่งอื่น ๆ

สุดท้ายคืออินเทอร์เน็ตไฟร์วอลล์ไม่สามารถปกป้องการโจมตีที่มากับข้อมูล (data driven attack) การโจมตีที่มากับข้อมูลเกิดขึ้นเมื่อข้อมูลที่ดูเหมือนไม่มีอันตรายถูกส่งมาทางเมล์หรือถูกคัดลอกไปยังโฮสต์ภายในและถูกเรียกใช้งาน ทำให้เกิดการโจมตี ตัวอย่างเช่น การโจมตีที่มากับข้อมูลอาจเป็นเหตุให้โฮสต์เปลี่ยนแปลงไฟล์ที่เกี่ยวข้องกับการรักษาความปลอดภัย ทำให้ง่ายขึ้นสำหรับผู้บุกรุกที่จะเข้าถึงระบบ การจัดให้มีพรอกซีเซอร์ฟเวอร์ไว้บนแบสชันโฮสต์เป็นวิธีที่ดีเยี่ยมในการห้ามไม่ให้มีการเชื่อมต่อโดยตรงจากภายนอก และลดการก่อกวนจากการโจมตีที่มากับข้อมูล

กล่องเครื่องมือของแฮกเกอร์

เป็นเรื่องยากที่จะบรรยายถึงการโจมตีของแฮกเกอร์ เนื่องจากผู้บุกรุกมีระดับแตกต่างกันตามความเชี่ยวชาญด้านเทคนิค และมีแรงผลักดันที่ต่างกันมากมาย แฮกเกอร์บางคนชอบความท้าทาย บางคนแค่ต้องการทำให้ชีวิตยุ่งยากกว่าคนอื่น และยังมีบางคนขโมยข้อมูลเพื่อแสวงหากำไร

การรวบรวมข้อมูล

โดยทั่วไปขั้นตอนแรกในการเจาะระบบคือการรวบรวมข้อมูล จุดประสงค์คือเพื่อสร้างฐานข้อมูลเครือข่ายขององค์กรเป้าหมาย และรวบรวมข้อมูลเกี่ยวกับโฮสต์ที่ตั้งอยู่บนส่วนต่าง ๆ ของเครือข่าย มีเครื่องมือจำนวนมากที่แฮกเกอร์สามารถเลือกใช้เพื่อเก็บรวบรวมข้อมูลนี้ เช่น

- โปรโตคอล SNMP สามารถนำมาใช้เพื่อตรวจดูตารางการจัดเส้นทาง (routing table) ของเราเตอร์ที่ไม่รักษาความปลอดภัย เพื่อเรียนรู้รายละเอียดเกี่ยวกับโทโปโลยีของเครือข่ายขององค์กรเป้าหมาย
- โปรแกรม TraceRoute สามารถเปิดเผยหมายเลขเครือข่ายและเราเตอร์ในเส้นทางไปสู่โฮสต์ที่ระบุ
- โปรโตคอล Whois เป็นบริการข้อมูลชนิดหนึ่งที่สามารถให้ข้อมูลเกี่ยวกับ DNS domain ทั้งหมดและผู้ดูแลระบบที่รับผิดชอบแต่ละโดเมน อย่างไรก็ตาม ข้อมูลนี้มักจะล้าสมัย
- เซอร์ฟเวอร์ DNS สามารถเข้าถึงรายการ IP แอดเดรสของโฮสต์และชื่อโฮสต์ที่ตรงกันได้
- โปรโตคอล Finger สามารถเปิดเผยข้อมูลในรายละเอียดเกี่ยวกับผู้ใช้ (ชื่อล็อกอิน หมายเลขโทรศัพท์ เวลาที่ล็อกอินครั้งสุดท้าย เป็นต้น) ของโฮสต์ที่ระบุได้
- โปรแกรม Ping สามารถนำมาใช้เพื่อค้นหาตำแหน่งโฮสต์ที่ต้องการและตรวจสอบการเข้าถึงได้ เครื่องมือง่าย ๆ นี้สามารถใช้ในโปรแกรมตรวจผ่านที่ ping ทุกโฮสต์แอดเดรสที่เป็นไปได้บนเครือข่าย เพื่อสร้างรายการของโฮสต์ที่มีอยู่จริงบนเครือข่าย

การสำรวจจุดอ่อนในการรักษาความปลอดภัยของระบบ

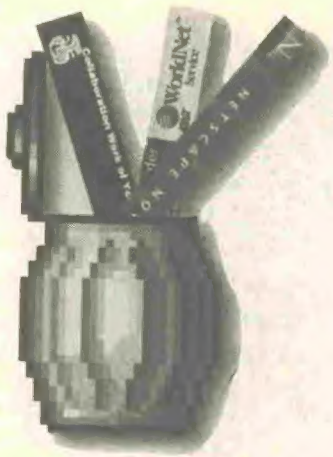
หลังจากรวบรวมข้อมูลเกี่ยวกับเครือข่ายขององค์กรเป้าหมายแล้ว แฮกเกอร์จะพยายามสำรวจจุดอ่อนในการรักษาความปลอดภัยของแต่ละโฮสต์ มีเครื่องมือจำนวนมากที่แฮกเกอร์สามารถใช้เพื่อตรวจโฮสต์แต่ละตัวบนเครือข่ายโดยอัตโนมัติ ตัวอย่างเช่น

- เนื่องจากบริการที่มีจุดอ่อนซึ่งเป็นที่รู้กันมีอยู่ไม่มาก แฮกเกอร์ที่มีความรู้จึงสามารถเขียนโปรแกรมขนาดเล็กที่พยายามเชื่อมต่อกับพอร์ตของบริการที่กำหนดบนโฮสต์เป้าหมาย เอาต์พุตของโปรแกรมคือรายการโฮสต์ที่สนับสนุนบริการนั้นซึ่งเปิดกว้างต่อการโจมตี
- มีเครื่องมือที่ใช้กันทั่วไปหลายตัว เช่น Security Administrator Tool for Anayging Networks (SATAN) ที่ตรวจสอบโดเมนหรือเครือข่ายย่อย (subnetwork) ทั้งหมดและค้นหาจุดอ่อนในการรักษาความปลอดภัย โปรแกรมเหล่านี้ระบุจุดอ่อนของแต่ละระบบซึ่งอาจถูกโจมตีได้ในหลาย ๆ จุด ผู้บุกรุกใช้ข้อมูลที่รวบรวมจากการตรวจสอบเหล่านี้เพื่อเข้าถึงระบบขององค์กรเป้าหมายโดยไม่ได้รับอนุญาต

ผู้ดูแลระบบที่เฉลียวฉลาดสามารถใช้เครื่องมือเหล่านี้ภายในเครือข่ายส่วนตัวของพวกเขาเพื่อค้นหาจุดอ่อนในการรักษาความปลอดภัย และตรวจดูว่าโฮสต์ใดต้องได้รับการปรับปรุงด้วยซอฟต์แวร์ที่แก้ไขใหม่

การเข้าถึงระบบที่ได้รับการปกป้อง

ผู้บุกรุกใช้ผลจากการสำรวจโฮสต์เพื่อกำหนดเป้าหมายที่จะโจมตี หลังจากเข้าถึงระบบที่ได้รับการปกป้องได้แล้ว แฮกเกอร์จะมีทางเลือกมากมาย เช่น



- ผู้บุกรุกอาจพยายามทำลายหลักฐานของการกระทำความผิด และเปิดช่องโหว่ใหม่ในระบบรักษาความปลอดภัย หรือเปิดประตูหลังในระบบเพื่อให้สามารถเข้าถึงได้ต่อไปแม้ว่าการโจมตีครั้งแรกจะถูกตรวจพบ
- ผู้บุกรุกสามารถติดตั้งแพคเก็ตสนิฟเฟอร์ (packet sniffer) ซึ่งรวมไว้ด้วยไบนารีของม้าโทรจัน (Trojan hourse) ที่ซ่อนเร้นกิจกรรมของตัวมันบนระบบนั้น แพคเก็ตสนิฟเฟอร์จะรวบรวมชื่อบัญชีและรหัสผ่านสำหรับบริการ Telnet และ FTP ที่ทำให้แฮกเกอร์ขยายการโจมตีไปสู่เครื่องอื่นได้
- ผู้บุกรุกสามารถค้นหาโฮสต์อื่นที่พึ่งพาระบบนี้ ทำให้แฮกเกอร์สามารถใช้ประโยชน์จากจุดอ่อนของโฮสต์เดียวและขยายการโจมตีไปทั่วทั้งเครือข่ายขององค์กร
- ถ้าแฮกเกอร์สามารถได้สิทธิในการเข้าถึงระบบ เขาหรือหล่อนสามารถอ่านเมล์ ค้นไฟล์ส่วนตัว ขโมยไฟล์ส่วนตัว และทำลายหรือทำให้ข้อมูลสำคัญเสียหาย

เรียนรู้เพิ่มเติมเกี่ยวกับการโจมตีทางอินเทอร์เน็ต

สำหรับข้อมูลล่าสุดเกี่ยวกับการโจมตีบนอินเทอร์เน็ต ติดต่อได้ที่ Computer Emergency Response Team (CERT) Coordination Center CERT ตีพิมพ์คำเตือนและสรุปเป็นระยะเพื่อดึงความสนใจไปที่การโจมตีหลากหลายชนิดซึ่งได้รับรายงานเข้ามา รายงานเหล่านี้ยังบรรจุข้อมูลและวิธีแก้ไขเพื่อเอาชนะการโจมตีแต่ละชนิด ไฟล์ใหม่หรือล่าสุดมีให้สำหรับ anonymous FTP จาก ftp://info.cert.org/pub/cert_summaries

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับเทคนิคที่ใช้โดยแฮกเกอร์ ติดตามได้จากกลุ่มข่าวของ USENET ที่ comp.security.announce, comp.security.mis, comp.security.unix, alt.2600, alt.wired, alt.hackers, และ alt.security สุดท้ายให้ค้นหาจาก bullatin board ของแฮกเกอร์ซึ่งมีอยู่ทั่วไป ตัวอย่างเช่น เซอร์ฟเวอร์ Telnet คอยฟังการเชื่อมต่อจากรีโมทบนพอร์ต TCP หมายเลข 23 และเซอร์ฟเวอร์ SMTP คอยฟังการเชื่อมต่อที่เข้ามาบนพอร์ต TCP หมายเลข 25 เพื่อที่จะปิดกั้นการเชื่อมต่อ Telnet ที่เข้ามาทั้งหมด เราเตอร์ก็เพียงแค่ทิ้งแพคเก็ตทั้งหมดที่บรรจุพอร์ต TCP ปลายทางมีค่าเท่ากับ 23 หรือเพื่อจำกัดการเชื่อมต่อ Telnet ไปยังโฮสต์ภายในจำนวนจำกัด เราเตอร์ต้องปฏิเสธแพคเก็ตทั้งหมดที่บรรจุพอร์ต TCP ปลายทางเท่ากับ 23 และไม่ได้บรรจุ IP แอดเดรสปลายทางของโฮสต์ที่ได้รับอนุญาต

กฎเกณฑ์ทั่วไปบางส่วนได้แก่

- อนุญาตให้ Telnet เข้ามายังโฮสต์ภายในที่กำหนดเท่านั้น
- อนุญาตให้ FTP เข้ามายังโฮสต์ภายในที่กำหนดเท่านั้น
- อนุญาตให้ Telnet ออกไปภายนอกได้ทั้งหมด
- อนุญาตให้ FTP ออกไปภายนอกได้ทั้งหมด
- ปฏิเสธการจราจรของข้อมูลทั้งหมดที่เข้ามาจากเครือข่ายภายนอกที่กำหนด

ข้อตัดสินในการออกแบบไฟร์วอลล์เบื้องต้น

เมื่อออกแบบอินเทอร์เน็ตไฟร์วอลล์ ผู้ดูแลเครือข่ายมีสิ่งที่ต้องตัดสินใจ ดังนี้

● จุดยืนของไฟร์วอลล์

● นโยบายการรักษาความปลอดภัยโดยรวมขององค์กร

● ค่าใช้จ่ายของไฟร์วอลล์

● ชิ้นส่วนหรือส่วนประกอบของระบบไฟร์วอลล์

จุดยืนของไฟร์วอลล์

จุดยืนของระบบไฟร์วอลล์พรรณนาถึงปรัชญาการรักษาความปลอดภัยพื้นฐานขององค์กร อินเทอร์เน็ตไฟร์วอลล์อาจมีจุดยืนที่ต่างกันโดยสิ้นเชิงหนึ่งในสองอย่างต่อไปนี้

● *ทุกสิ่งที่ไม่ได้รับอนุญาตเป็นพิเศษจะถูกปฏิเสธ* จุดยืนนี้อยู่บนสมมติฐานที่ว่าไฟร์วอลล์ควรปิดกั้นการจราจรของข้อมูลทั้งหมด และบริการหรือแอพพลิเคชันที่ต้องการควรถูกดำเนินการเป็นกรณีไป นี่คือวิธีที่แนะนำ สภาวะแวดล้อมที่สร้างขึ้นจะมีความปลอดภัยมาก เนื่องจากบริการที่ถูกคัดเลือกอย่างระมัดระวังเท่านั้นที่ได้รับการสนับสนุน ข้อเสียคือมันเน้นการรักษาความปลอดภัยมากกว่าความง่ายในการใช้งาน จึงมีตัวเลือกให้กับสังคมของผู้ใช้จำนวนจำกัด

● *ทุกสิ่งที่ไม่ได้ถูกปฏิเสธเป็นพิเศษจะได้รับอนุญาต* จุดยืนนี้อยู่บนสมมติฐานที่ว่าไฟร์วอลล์ควรส่งต่อการจราจรของข้อมูลทั้งหมด และบริการที่อาจมีอันตรายควรถูกปิดเป็นกรณีไป วิธีนี้สร้างสภาวะแวดล้อมที่ยืดหยุ่นมาก พร้อมกับมีบริการให้กับสังคมของผู้ใช้มากกว่า ข้อเสียคือมันเน้นความง่ายในการใช้งานมากกว่าการรักษาความปลอดภัย ผู้ดูแลเครือข่ายจึงรู้สึกต่อต้าน และทำให้ยากขึ้นที่จะรักษาความปลอดภัยเมื่อขนาดของเครือข่ายที่ได้รับการปกป้องขยายขึ้น

นโยบายการรักษาความปลอดภัยขององค์กร

ดังที่กล่าวมาแล้วว่าอินเทอร์เน็ตไฟร์วอลล์ไม่ได้ยืนโดยลำพัง มันเป็นส่วนหนึ่งของนโยบายการรักษาความปลอดภัยโดยรวมขององค์กร ซึ่งกำหนดแนวป้องกันทุก ๆ ด้าน การที่จะประสบความสำเร็จองค์กรต้องรู้จักสิ่งที่พวกเขากำลังปกป้อง นโยบายการรักษาความปลอดภัยต้องตั้งอยู่บนการวิเคราะห์ระบบรักษาความปลอดภัย การประเมินความเสี่ยง และการวิเคราะห์ความต้องการของธุรกิจ ทั้งหมดนี้ต้องถูกควบคุมอย่างรอบคอบ ถ้าองค์กรไม่มีนโยบายการรักษาความปลอดภัยในรายละเอียด ไฟร์วอลล์ที่รอบคอบที่สุดก็สามารถถูกหลีกเลี่ยงเพื่อจะเปิดกว้างเครือข่ายส่วนตัวให้กับการโจมตีได้

ค่าใช้จ่ายของไฟร์วอลล์

การรักษาความปลอดภัยขนาดไหนที่องค์กรสามารถจ่ายได้ ? ไฟร์วอลล์แบบกรองแพคเก็ต (packet-filtering) อย่างง่ายอาจมีค่าใช้จ่ายต่ำที่สุดเนื่องจากองค์กรต้องการเราเตอร์ตัวหนึ่งต่อกับอินเทอร์เน็ต และการกรองแพคเก็ตถูกรวมเป็นส่วนหนึ่งในคุณสมบัติของเราเตอร์มาตรฐาน ระบบไฟร์วอลล์ในทางการค้าให้ความปลอดภัยมากขึ้น แต่อาจมีค่าใช้จ่ายตั้งแต่ U.S.$4,000 ถึง U.S.$30,000 ขึ้นอยู่กับความซับซ้อนของมันและจำนวนของระบบที่ได้รับการปกป้อง ถ้าองค์กรมีผู้เชี่ยวชาญเอง ไฟร์วอลล์อาจสร้างขึ้นได้เองจากซอฟต์แวร์สาธารณะ แต่ก็ยังคงมีค่าใช้จ่ายในรูปของเวลาที่ใช้พัฒนาและจัดระบบไฟร์วอลล์ ท้ายที่สุดไฟร์วอลล์ทั้งหมดต้องการการสนับสนุนอย่างต่อเนื่องสำหรับการบริหาร การบำรุงรักษาทั่วไป การปรับปรุงซอฟต์แวร์ การแก้ไขในด้านความปลอดภัย และการรับมือกับเหตุการณ์ที่ไม่คาดคิด

ส่วนประกอบของระบบไฟร์วอลล์

หลังจากทำการตัดสินใจเกี่ยวกับจุดยืนของไฟร์วอลล์ นโยบายการรักษาความปลอดภัย และงบประมาณที่ต้องใช้ องค์กรสามารถกำหนดเลือกส่วนประกอบที่ต้องการของระบบไฟร์วอลล์ ไฟร์วอลล์ทั่วไปประกอบด้วยส่วนประกอบส่วนหนึ่งหรือหลายส่วนต่อไปนี้

● เราเตอร์แบบกรองแพคเก็ต (Packet-filtering router)

● เกตเวย์ระดับแอพพลิเคชัน (Application-level gateway) หรือพรอกซีเซอร์ฟเวอร์ (proxy server)

● เกตเวย์ระดับวงจร (Circuit-level gateway)

สรุป

ไม่มีคำตอบที่ถูกเพียงคำตอบเดียวสำหรับการออกแบบและใช้งานอินเทอร์เน็ตไฟร์วอลล์ การตัดสินใจของแต่ละองค์กรจะขึ้นอยู่กับปัจจัยหลายอย่างแตกต่างกัน เช่น นโยบายการรักษาความปลอดภัยของบริษัท พื้นฐานทางเทคนิคของพนักงาน ค่าใช้จ่าย และการคุกคามจากการโจมตีที่รับรู้ บทความนี้เน้นในหลายประเด็นที่เกี่ยวกับการสร้างอินเทอร์เน็ตไฟร์วอลล์ รวมทั้งประโยชน์ของพวกมัน ข้อจำกัด ส่วนประกอบ และตัวอย่างของระบบไฟร์วอลล์ เนื่องจากประโยชน์ของการเชื่อมต่อเข้ากับอินเทอร์เน็ตส่วนกลางอาจอยู่เหนือค่าใช้จ่าย ผู้จัดการเครือข่ายควรเดินหน้าต่อไปด้วยความระแวดระวังอันตราย และการทำความเข้าใจ ว่าด้วยการป้องกันล่วงหน้าอย่างถูกต้อง เครือข่ายของพวกเขาจะปลอดภัยได้มากเท่าที่พวกเขาต้องการให้มันเป็น